**INTERCEPTLS**

Detection and Characterization of TLS Interception in Access Networks

**Motivation**

- TLS connections are intercepted [1, 2, 3]
- These interceptions were detected using a single viewpoint approach (either client or server viewpoint)
- Single viewpoint approaches rely on heuristics or may not detect all interceptions
- Our goal is to detect interceptions and characterize middleboxes to obtain a more complete picture (client and server side view), e.g. detect selective interceptions

**Background**

- Transport Layer Security (TLS) is used to establish a secure connection between two parties
- Trust is established via Public Key Infrastructure (PKI)

![TLS handshake protocol messages](image)

**Design**

- Obtain full picture of TLS interceptions (client and server view)
- Detect (selective) interceptions
- Characterize middlebox (supported TLS versions, mimicked TLS fingerprint, behaviour on non-existent server name identification or http host)
- Obtain network information (network type, public ip address, gateway, DNS, location)
- Crowd-sourced approach (Android app and desktop client)

**Implementation**

Clients are available for:

- Android (6.0+)
- CLI (tested on Ubuntu 17.10, macOS 10.13)

**Results**

In four months, 3485 measurements were collected. Four of these were intercepted using self-signed certificates. Further analysis is still required.

**Future Work**

- Support for TLS 1.3
- Deploy server in different environments
- Grow user base
- Add additional middlebox characteristics

Support us and download the Android app. More information about the project can be found on [https://interceptls.net.in.tum.de](https://interceptls.net.in.tum.de)

---